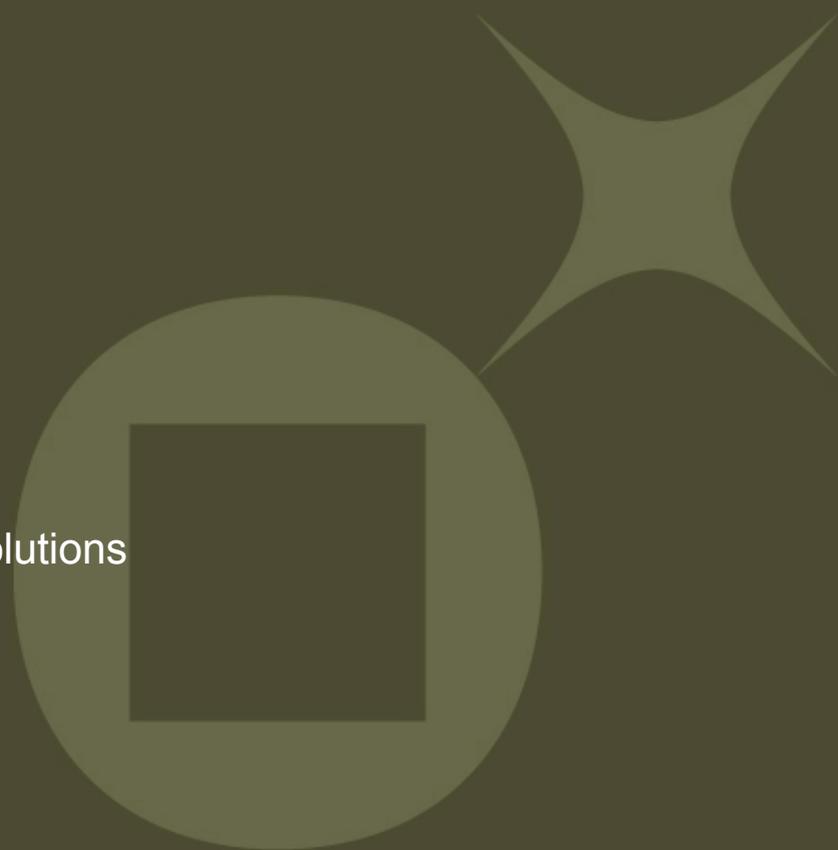


智能卡 助力企业数字信息安全

马志民

Gemalto – ID & Security Solutions
Sep 2006



议程

✦ Gemalto

✦ 企业安全

- 身份管理的挑战
- 身份认证及用户管理: **SafesITe** “解决方案”
- 案例学习

安全领域的专家

安全是智能卡技术的基本特征

- ✦ 行业内最大,最有经验的团队和加密专家
 - 顾问, 审核, 方案设计及支持
 - 持续的系统升级
- ✦ 我们涉足于智能卡安全领域的每一个角落
 - 密码学, OS 安全, Internet及网络安全, 工程实践, 防止篡改、抵赖, 认证及风险管理
 - 卡体材料和可视安全特征
 - 个人化系统和处理
- ✦ 我们不断创新并提供客户所需的产品

我们的核心业务

- ✦ 我们设计具有高安全性的卡片操作系统
- ✦ 我们制造模块和卡片,卡体有多种材质和安全特征
- ✦ 我们设计并制造读卡器界面、读卡器、读卡器芯片
- ✦ 我们提供全套的软件、中间件、以及完整的企业安全解决方案
- ✦ 我们提供个人化系统以及卡片管理系统
- ✦ 我们提供完整的顾问、设计、培训、安装、支持服务



网络的风险

✦ IT 网络是非常敏感的

- Intranets & VPNs 是公司发展的必经之路
- Internet 的使用迅猛增长
- 远程及动态连接: wireless, mobile workers, telecommuters...
- 重要的信息存储于网络之上

✦ Hacker潜伏在网络上

- 由于高额回报，网络欺诈逐渐增多。
- 网络信息被人监控

✦ 增加了财务和法律信息的风险

- 网络服务的中断直接导致客户流失
- 又可能导致更多的经济处罚

新的需求

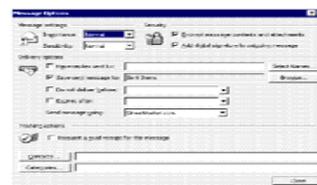
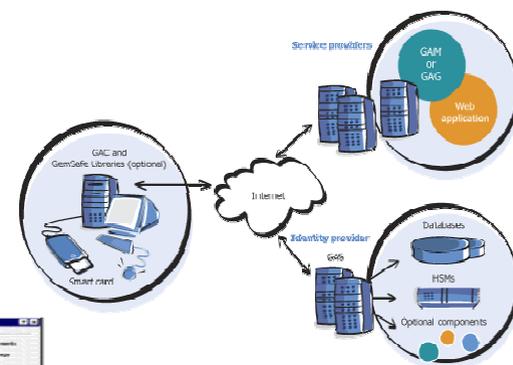
◆ 门禁的保证



◆ 安全控制接入网络 Secure access to networks

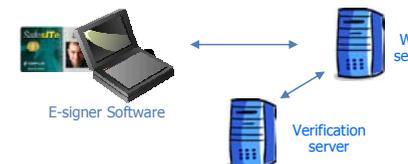
◆ 控制应用的使用 Secure access to applications

◆ 应用的加密 Run secure applications



email

Internet



Digital signature



为什么需要身份认证管理

✦ 身份认证: 对员工、集团

- 员工需要进入办公室、计算机、公司网络的认证
- 集团需要建立一个安全的信息共享平台

✦ 身份安全已经成为公司业务发展的一个重要策略

- 保护公司网络上的重要信息不被泄密
- 安全连接IT系统，商务伙伴，供应商，客户
- 增加不断增多的客户需求

✦ 有效的身份认证管理会降低公司成本

- 可以减少安全管理的成本
- 尽可能减少被恶意攻击的损失
- 员工专职于工作，不必为网络安全担忧

身份认证管理结构



为什么使用身份管理 保护在线交易

★ 数字签名，用于交易和文件

- 符合国内、国际标准 → 法律认可
 - 欧洲: Digital Signature Directive (Dec 1999)
 - 美国: Electronic Signatures Act (July 2000), E-Sign (October 2000)
 - 其他国家, 拉美 (巴西, 阿根廷, 智利...), 亚洲 (中国, 新加坡, 马来西亚...)
- 双因子鉴全
 - 你有什么: token 或者智能卡
 - 你知道什么: PIN 码
- 一整套的应用
 - Email签名 (Outlook...), 表格 (PDF...)
 - 其他应用: time-stamping and archiving

★ B2B 和 B2C 方面

- B2B: 建立与供应商、客户、商业伙伴法律认可的在线的合约
 - 全球或直属网络
- B2C: 建立与客户在线, 可信任关系

★ 重要的商业回报

- 速度: 交易过程由几天缩减到几个小时
- 端到端的数字交易成为可能
- 在互联网上可以带来更多的市场机会

智能员工卡: 企业的最佳选择

★ 安全范例

- What you have: smart ID card
- What you know: PIN Code
- 可选 - : 生物特征



★ 通过芯片实现的硬件

- 密钥保存在于安全的受保护的载体中

★ 与现有门禁卡的兼容

- 兼容现有的非接触式技术
- 可以实现与现有系统的无缝整合

★ 实用并且方便

- 员工的照片和姓名可以打印在员工卡上
- 可以与信用卡结合
- 大多数的计算机开始内置读卡器

仅针对逻辑接入,
a chip-sized smart card
can be plugged...



...or molded...



...in a USB dongle.

智能卡是安全认证的最佳选择

Gem e-Seal



★ USB token

- 封装Java智能卡芯片，通过 CCEAL5+ 认证
- GemCore 智能卡界面
- USB 2.0
- PC/SC drivers
- Microsoft CCID compliant

★ 便携设备

- 只有钥匙大小 (LWH 64x16x8 mm)
- 防篡改封装
- 具备钥匙环设计
- 可定制颜色、logo



Gem e-Seal



GemPC Key



GemXpresso R3.2 32K
smart card chip

一个鉴权和用户管理的子系统

★ 鉴全推动用户管理

- 定义谁需要鉴全
- 为用户提供鉴全设备
- 管理鉴全周期

★ 管理一个完整的系统:

- 录入, 发行, 后个人化
- 客户端鉴全

★ 动态鉴全系统组成



Applet



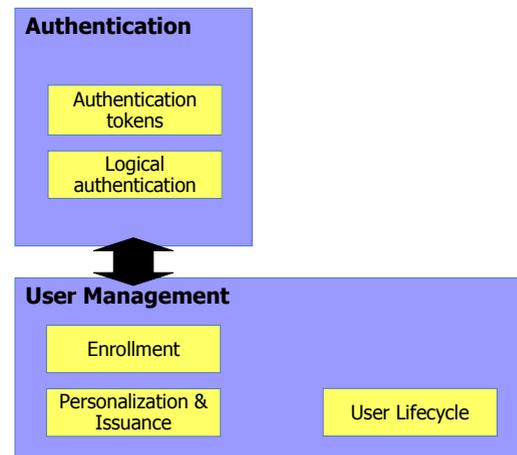
Middleware

Back-end



CMS

Card + Applet + Reader + Middleware + CMS



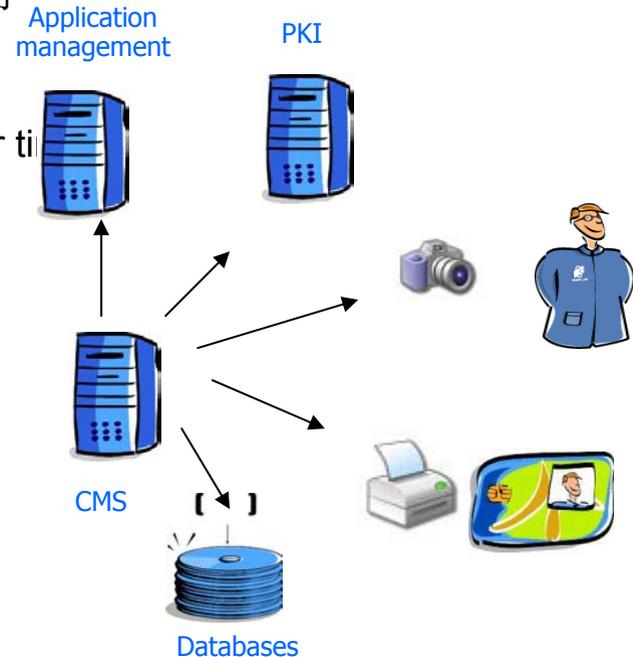
CMS 用于用户管理

✦ 卡片管理 (CMS) 管理卡片和安全数据的生命周期

- 生成个体卡片 **Create one card for one individual**
- 联接并通知系统 **Links to and informs legacy system**
- 不断更新数字身份 **Keep modifying this digital identity over ti**

✦ CMS 管理的不同步骤

- 发行并个人化智能员工卡
 - 录入员工信息, 更新 HR 数据库
 - 密钥、证书、属性 **Keys and certificates, attributes**
 - 卡体图案和逻辑数据 **Graphical and logical data**
- 卡片生命周期管理 **Card life-cycle management**
 - 卡片遗失, 忘记 PIN, ,...
 - 修改/更新权限
 - 删除/更新应用
- 证书生命周期管理
- 再更新应用和数据



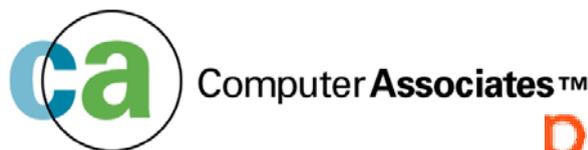
✦ Gemalto' SafesITe smart ID Card Manager offer

- 模块化的方案适用于不同需求

我们的合作伙伴

★ SafesITe 适用于各种产品和技术

- Single Sign On solutions
- Virtual Private Network
- CA认证
- 个人化设备



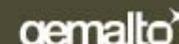
CISCO SYSTEMS



CHECK POINT



HID CORPORATION



我们的客户群

	行业	Gemplus 客户
B2B	银行和其他	Barclays (UK), HBOS (UK) HSBC (UK)... ICBC (China) BRED (FR) Standard Chartered (SG) Omel (SP)
员工卡	健康和医疗	Denver Healthcare (US) Queens Health Network Pfizer (US)
	银行	ABN-Amro (NL) Barclays (UK)
	其他	Boeing (US) Telefonica Data (Peru)
	政府	UK Dpt of Work and Pensions



中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA



HSBC



BARCLAYS



oemalto^x

案例

波音公司智能员工卡

✦ 方案由业界领先者共同完成

- Gemalto: 智能卡业的领导者
- Siemens: 最大的系统集成商

✦ SafesITe 达到了需求和安全的要求

- 智能卡, 64KB, Java, 带有 GemSafe applets
- 读卡器: 外置和笔记本专用(PCMCIA)
- GemSafe 客户端软件
- BellID CMS

✦ 项目部署

- 这是在美国最大的集团智能员工卡项目
- 目前已发放80k张智能员工卡
- 新的应用还在添加
- 扩展到更多的商业伙伴

Thank You

www.gemalto.com

